Aalto University
School of Economics

Economic and Institutional Implications of Blockchain

Master's thesis

Henrik Suikkanen

16/9/2017

Economics

Approved by the Head of the Economics Department __.__.2017 and awarded the grade

1._____ 2. _____

Author Henrik Suikkanen

Title of thesis Economic and Institutional Implications of Blockchain

Degree Master of Science in Economics and Business Administration

Degree program Economics

Thesis advisor Mikko Mustonen

Year of approval 2017 **Number of pages** 55 **Language** English

Abstract

Blockchain technology has been raising enthusiasm over a variety of disciplines, from information technology and finance, to law and economics. Blockchain is a decentralized ledger, which facilitates trust and makes peer-to-peer transactions possible without a central third-party authority. Since 2008, cryptocurrency bitcoin has provided an example of how to implement a marketplace without a central authority by using blockchain technology. The fact that a broad range of economic and government activities rely on a centralized recording of the basic data of the economy makes this technology potentially significant. The utopian views of blockchain have argued that it will disrupt a wide range of markets by eliminating the need for intermediation.

The objective of this thesis is to review the relevant literature related to the topic and provide a guide to what blockchain means in the field of economics. The published research is mapped through a three stage literature review, and based on this, it is organized in three main categories: monetary-, innovation- and governance-centred research.

Even though the literature surrounding the topic is still in its infancy, the potential of blockchain technologies is recognized by the literature. From the monetary viewpoint blockchain gives unprecedented flexibility in designing the attributes of currencies in terms of supply, value and exchange. From the innovation viewpoint, blockchain can create both increased efficiency of existing markets but also profits through entirely new markets. From the governance viewpoint blockchain facilitates trust and can be instrumental in democratizing economy more towards peer-to-peer production and consumption.

Rather than a single technology, blockchain should be understood as a part of a greater digital transformation. In this case, blockchain can play a role in unlocking the potential of digital commons as well as the sharing and platform economy through a decentralized, universal record-keeping system.

Keywords Blockchain, Bitcoin, Distributed Ledger Technologies, Cryptocurrency, Moneteary Economics, New Institutional Economics, Economics of Innovation

Tekijä Henrik Suikkanen

Työn nimi Economic and Institutional Implications of Blockchain

Tutkinto Kauppatieteiden maisteri

Koulutusohjelma Taloustiede

Työn ohjaaja Mikko Mustonen

Hyväksymisvuosi 2017 **Sivumäärä** 55 **Kieli** englanti

Tiivistelmä

Lohkoketju (blockchain) on herättänyt kiinnostusta useilla tieteenaloilla, aina informaatioteknologiasta ja rahoituksesta oikeus- ja taloustieteeseen. Kyseessä on hajautettu tietokanta, joka välittää luottamusta verkon yli ja mahdollistaa transaktiot ilman keskitettyä kolmatta osapuolta. Vuodesta 2008 eteenpäin kryptovaluutta bitcoin osoitti, että markkinapaikan luominen ilman kolmatta luotettua osapuolta on mahdollista lohkoketjun avulla. Lohkoketjusta potentiaalisesti merkittävän teknologian tekee se, että valtaosa taloudellisista ja hallinnollisista toiminnoista perustuu keskitettyihin tietokantoihin. Utopistisimmat näkökulmat lohkoketjuun väittävätkin sen mullistavan laajan joukon markkinoita poistamalla tarpeen kolmansille osapuolille.

Tämän tutkielman tavoite on käydä läpi taloustieteen näkökulmasta oleellinen lohkoketjua koskeva kirjallisuus ja tarjota siten yhteenveto, mitä lohkoketju potentiaalisesti tarkoittaa taloustieteessä. Julkaistu lohkoketjua käsittelevä taloustieteen tutkimus kartoitetaan kolmivaiheisen kirjallisuuskatsauksen kautta sekä jaetaan tämän perusteella kolmeen pääkategoriaan: raha-, innovaatio- ja hallintokeskeiseen tutkimukseen.

Vaikka lohkoketjua käsittelevä kirjallisuus on vasta alkutekijöissään, teknologian potentiaali on selkeästi tunnistettu. Rahataloustieteen näkökulmasta erityisen kiinnostavaa on se, että lohkoketju avaa ennennäkemättömän joustavuuden digitaalisen rahan suunnittelussa. Innovaatiokeskeisestä näkökulmasta lohkoketju puolestaan oletettavasti sekä tehostaa nykyisten markkinoiden toimintaa että luo kokonaan uusia markkinoita. Hallinnollisesta näkökulmasta lohkoketju välittää luottamusta ja edesauttaa talouden demokratisoitumista kohti vertaistuotantoa -kulutusta.

Yksittäisen teknologian sijaan lohkoketju tulee ymmärtää osana suurempaa muutosta kohti digitaalista taloutta ja yhteiskuntaa. Tässä tapauksessa lohkoketjulla voi olla merkittävä rooli niin digitaalisten yhteisten resurssien hyödyntämisessä kuin myös jakamis- ja alustatalouden potentiaalin realisoimisessa universaalin ja hajautetun kirjanpitojärjestelmän myötä.

Avainsanat Lohkoketju, bitcoin, hajatuettu tietokanta, kryptovaluutta, rahataloustiede, uusi institutionaalinen taloustiede, innovaatiotaloustiede

Acknowledgements

I have been fortunate to receive support from many thoughtful people throughout the writing process. I would like to thank especially my supervisor Mikko Mustonen for showing genuine interest towards my work and providing materials and support from the very beginning. This has been an important part of my motivation. I also highly appreciate the comments I have got from ReCon's research team. Finally, I would like to thank my friends, especially Niklas Håkansson, for numerous interesting conversations around the topic, Kira Keini and Johanna Suikkanen for helping in finalizing the work, and the rest of my family for providing support throughout the process.

Key Concepts

Blockchain = decentralized ledger of records and transactions (defined more specifically in chapter 3)

Ledger = collection of transactions and accounts

Blockchain network = network of peers who are using and maintaining the blockchain network

Mining = the procedure through which new information is added to the blockchain and new digital money is issued

Bitcoin = decentralized digital currency, i.e. cryptocurrency, that runs on the blockchain technology

Digital Currency = digital representation of value

Cryptocurrency = a digital currency that does not need any intermediaries in order to perform electronic transactions

Contents

List of Figures

1 Introduction

The blockchain technology has been raising enthusiasm over a variety of disciplines, from information technology and finance, to law and economics. Blockchain became known as the backbone technology for the cryptocurrency bitcoin. However, blockchain is much more than just the innovation behind bitcoin. It is a decentralized ledger enabling peer-to-peer transactions among people who have no particular trust on each other. It is certainly one of the most interesting recent technological developments due to its potentially disruptive features.

The significance of this new technology lies in the fact that a broad range of economic activities rely on centralized, agreed-upon recording of basic data of the economy: registries of assets, exchange, identities, contracts, value and so on. So far, the governance and authentication of this information has been reliant on centralized systems, including banks, firms, and governmental institutions. However, blockchain has proved its potential to facilitate exchange and disseminate trust without a neutral third-party authority. Established in 2008, bitcoin has been the first example of how to implement a marketplace without a central authority through blockchain technology. Since then, blockchain has gained attention due to its potential impact on the ways to organize information and interactions of groups of people.

Blockchain is becoming a buzzword due to lack of clear terminology, making it hard to construct a comprehensive picture of the phenomenon. The utopian views of blockchain have argued that it will disrupt all markets by eliminating the need for intermediation. More realistically, Catalini and Gans (2016) argue that blockchain is "more likely to change the scope of intermediation" through reduction of transaction costs and by allowing new types of marketplaces to emerge. Altogether, there is a need for a clearer conceptualization of what blockchain means in the field of economics, and for understanding what the possible economic and institutional implications of this new technology are.

1.1 (De)centralization

Adam (1759) argued that open and decentralized systems lead to evolutionary efficiency in complexity. However, systems tend to centralize for several reasons. First, the centralization of governance improves efficiency in establishing and enforcing rules and solving disputes. Second, a neutral centralized third-party intermediary disseminates trust between economic agents. Third, centraliza-

tion eases the accumulation of knowledge, creating knowledge structures and enabling scale economies. Fourth, centralization simplifies the coordination of actions, and thereby prevents unnecessary duplication.

As centralized systems grow in size and complexity, they become inefficiently expensive. Large and complex centralized systems are less resilient, robust, flexible, secure and efficient. The marginal cost of centralization increases as complexity and scale grow.

Blockchain is a technology for crating trust and consensus of records and transactions, which are instrumental to economic coordination. This could make decentralization relatively efficient compared to centralization. Blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority.

1.2 Research Objectives and Research Question

This thesis provides an overview and analysis of the relevant published work related to the topic and to provide a guide to what blockchain means in the field of economics. The overview can be used by academia and decision-makers as an up-to-date report on the current state of the field. It can also make it easier for further researchers to construct a comprehensive picture of the topic.

The main research question of this thesis is: *"What are the possible economic and institutional implications of blockchain?"*

1.3 Structure of the Thesis

The thesis starts with an overview of the literature review. Chapter 3 defines what blockchain means in the field of economics. Chapters 4, 5 and 6 summarize, discuss and interpret each of the three approaches, monetary-, innovation- and governance-centred approaches. Chapter 7 summarizes and discusses the findings and suggests directions for the future research.

2 Overview of the Literature

The objective of this literature review is to give an overview of the published literature related to the economics of blockchain and to assort and structure the literature in a meaningful way. Through a three-phase literature review process, the published literature of the subject area is organized in three main categories: monetary-, innovation- and governance-centred points of view. After this the material is synthesized, discussed and interpret.

2.1 Three Main Streams of the Research

After the three-stage review process, a logical approach was developed to group the main streams of the research.

2.1.1 Monetary-Centered Approach

According to Böhme et al. (2015), blockchain is of interest to economists due to its potential to disrupt existing payment systems and perhaps even monetary systems. As the cyptocurrency bitcoin is the most prominent and popular blockchain application, and the overall cryptocurrency market has recently exceeded the valuation of 80 billion USD (Coinmarketcap.com, 2017), it is no surprise that a majority of the blockchain literature discusses the financial and monetary implications of blockchain. Thereby, the monetary-centered approach is identified as one of the main streams of research. More specifically, monetary economics means for example reviewing the implications of blockchain on monetary systems, price levels and interrelations of nominal and real economy. These implications are reviewed and discussed in chapter 4.

2.1.2 Innovation-Centered Approach

According to Davidson et al. (2016a,b) there are two approaches to the meaning of technological change: the neoclassical approach and the new institutional approach. In the neoclassical approach technological change lowers production costs and firms are economizing on production costs, which leads to efficient allocation of resources. Thereby, the innovation-centred approach to blockchain examines the efficiency improvements of production and the technological change as a change in factor productivity. The innovation-centered approach is reviewed and discussed in chapter 5.

2.1.3 Governance-Centered Approach

In the new institutional approach, in turn, technological change improves the efficient use of institutions, like markets and firms (Davidson et al., 2016b). In this approach, blockchain is an innovation that could be used to create new ways of governance and coordination of groups of people. Whereas in the innovation-centered approach firms are economizing on production costs, in the governance-centered approach firms economisze on transaction costs of exchange, leading to efficient institutional structure of economic organization and governance. In practice, this refers to the implementation of the institutional environment and the functioning of for example the legal system, markets, firms and contracts. The governance-centered approach is reviewed and discussed in chapter 6.

3 What is Blockchain?

Shortly after the 2008 financial crisis, Satoshi Nakamoto 2008 published a whitepaper to introduce bitcoin: a cryptographic peer-to-peer digital money, i.e. cryptocurrency. An open protocol that solved the double-spending problem[1], which was the main obstacle in establishing a digital money, was called the *Block Chain*. Henceforth, the word blockchain has been evolving. Nowadays blockchain is associated with a certain type of open protocol which is used to implement marketplaces without the need for a central authority (Catalini and Gans, 2016).

At the high level, blockchain is a digital list of accounts and balances, like a ledger. Because a copy of the ledger is broadcasted to all nodes[2], a group of actors rather than a single entity is responsible for validating the changes in the ledger. The idea is that the shared blockchain ledger records every transaction that has ever occurred in the network and thus maintains the complete information of the accounts and balances of users. The complete information is used to verify for example transactions, ownerships, transaction histories, reputations, and so on. If there is a dispute what is the correct copy of the ledger and there is overlapping data of the previous transactions, the agreement – which is the correct copy of the ledger – is made without a central authority, through a distributed and incentivized consensus protocol.

The pioneer blockchain application, bitcoin, provided "the first example of how an open protocol can be used to implement a marketplace without a need for a central authority" Catalini and Gans (2016). The fact that a decentralized group of people, rather than a single entity, is maintaining the ledger is the reason why blockchain has also raised its popularity at the societal level (Mattila, 2016).

3.1 Definition of Blockchain

A formal, universally accepted and all-inclusive definition of blockchain does not yet exist. Due to the lack of clear terminology, the blockchain phenomenon can be very confusing to understand (Mattila, 2016). In this thesis, blockchain

[1]Double-spending refers to a situation where it is possible to spend a digital token twice if the files can be duplicated.

[2]Node refers to an active device that is capable of creating, receiving, or transmitting information over the blockchain network.

is defined more precisely through its three main features:

1. A digital ledger that is replicated across multiple sites.
2. The records in the ledger are time-stamped and chained together cryptographically.
3. A decentralized and incentivized decision-making process, i.e. a consensus protocol, is used to decide which copy of the ledger is correct.

All three features have a crucial role in implementing a decentralized architecture. First, the replication of the ledger across multiple sites allows each node to access the transaction history. This is a precondition for the transparent and decentralized nature of the blockchain network. Second, chaining the ledger's time-stamped entries cryptographically makes it tamper-proof and provides security since new transactions need to reference to the previous ones in order to be accepted. Third, a consensus protocol enables gaining a consensus of the chronology and contents of the ledger without a central authority. The third feature also distinguishes blockchain from close concepts like centrally governed cryptographic databases.

Altogether, blockchain is a combination of several existing inventions. Broadcasting a continuously growing ledger of transactions across a network of growing number of connections requires an increasing capacity of processing, storing and shipping information[3]. Even though the inventions are old, According to Davidson et al. (2016b), the reason why blockchain has become a viable technology only recently lies in the exponential decrease in the cost of processing, storing and shipping information.

3.1.1 Replication Across Multiple Sites

Blockchain consist of a tamper-proof history of all preceding transactions that have taken place in the network. This allows for each node to scroll backwards the transaction history and verify the correct accounts and balances. In contrast to a traditional centralized ledger, in blockchain a copy of the records is broadcasted across the network.
The main outcome of the replication is that if agent "Alice" is willing to transfer digital tokens to agent "Bob", she has to refer to the previous transaction history that she in fact is the owner of the token she is willing to transfer. Others

[3]Note Metcalfe's law: As new nodes joins a network, the number of unique connections in a network grows exponentially.

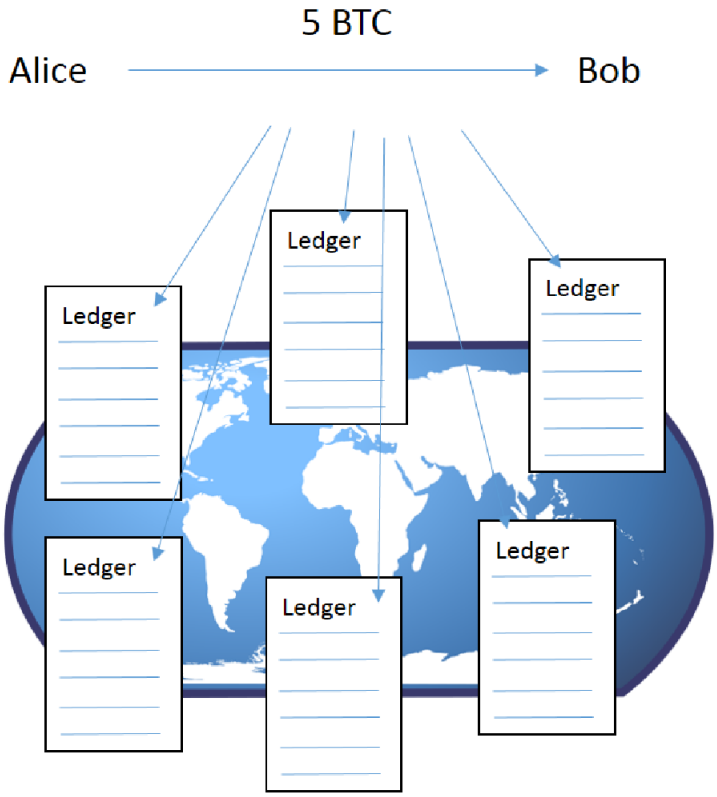

Figure 1: Broadcasting transactions across multiple sites

in the network can confirm this because they are able to access the transaction history. Once the network agrees about the transaction, the updated list of records is broadcasted again across the network (Figure 1).

3.1.2 Cryptographic Chain

Cryptographic protocols allow the transfer of sensitive information over a public network and prevent third parties from tampering the information (Bellare and Rogaway, 2005). The invention of digital signatures and timestamping in the 1970s provided premises for pure peer-to-peer digital currencies. Diffie and Hellman (1976) published a paper on a public-private key cryptosystem. This meant that enciphering and deciphering of data required two distinct keys: a public and a private one. Figure 2 illustrates the logic how the public-private

key cryptography works.

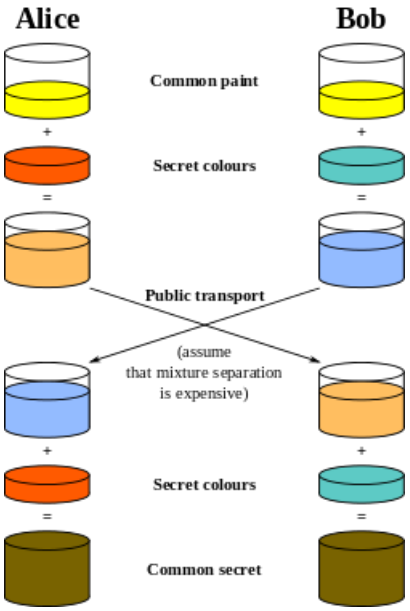

Figure 2: Diffie-Hellman Key Exchange (A.J. Han Vinck 2011)

In a blockchain network, a public-private key cryptography enables procedures that make the transactions tamper-proof, traceable and secure. The illustration in the figure 2 is a simplification but it encompasses an important feature: the solution to a problem is hard to find by outsiders, but once found, it is easy to check by others.

When the public transportation of information takes place, it is hard for an outsider to guess the "secret colours". However, as Alice and Bob decrypt the message with their secret colours and form the "common secret", it is easy for others to accept the original information (colours) that later on was mixed for the transfer.

For example, the bitcoin network works through SHA-256 cryptography. Each transaction has a unique and completely unpredictable 32-character long cryptographic hash function[4], i.e. a digital signature. The digital signature includes crucial information about the transaction, including user codes, transferable as-

[4]Cryptographic hash functions have an input (message) and an output (digest). In between there is a cryptographic hash function. It is easy to compute a hash value for any given message, but it is infeasible to generate a message from its hash value except by trying all possible messages. Thus the solution can be found only iteratively.

sets and timestamps. The information is encrypted behind the cryptographic protocol and its decryption and adding to the chain of preceding transaction requires using processing power by others in the network. Once the solution to the cryptographic hash function is found, i.e. the crucial information is decrypted, confirming it by others is easy. If the latest transaction is acceptable when referring to the preceding transaction in the network – or in other words, Alice had indeed had the funds that she sent to Bob – the transaction is added to the shared ledger.

3.1.3 Incentivized Consensus Protocol

Lastly, there are two crucial questions left: i) why would the rest of the blockchain network be interested in maintaining the blockchain by decrypting the transaction information (by spending some scarce resource like computing power) and ii) what happens if two or more nodes have an overlapping copy of the ledger? The solution is an incentivized consensus protocol. Consensus protocols are designed to keep the system running and to add the correct information to the ledger in a decentralized network of strangers. Thus, the network of nodes are able to maintain the blockchain. In the other words, consensus protocol is the way how everyone on the blockchain network can reach consensus in deciding together what data accurately represents recent transactions across the network.

The protocols are incentivized in such a way that the nodes ought to act according to the rules and add only correct information to the ledger. In practice, this would mean some sort of a "carrot-stick" system where the nodes are rewarded when they add information which a majority of the network agrees with[5]. Thereby, in order to tamper the ledger, a majority of the network should cooperate by claiming some false information to be correct. This should be against their own interests if the incentive to add the correct information is high enough compared to the possible gain of tampering the ledger. The reward is typically a valuable token, like bitcoins. This process is also used usually to supply more digital money to the system.

The most popular consensus protocol is proof-of-work (PoW), where nodes need to use their processing power to solve the cryptographic hash functions and thus validate the new blocks. Another popular consensus protocol is proof-of-stake (PoS), where the scarce resource to validate the transactions is some sort of a valuable stake. These can be digital tokens, for example. Alternative consensus

[5]Recall the feature of cryptographic hash functions: hard to solve but easy to check.

protocols are continuously developed.

Proof-of-Work

As explained earlier, cryptographic hash functions are used to create a unique digital signature for each transaction. This digital signature is broadcasted to the entire network and should be decrypted iteratively. By using computing power the nodes start to compete in solving the original input that created the digital signature. This happens by submitting randomly all possible inputs. The process is called mining.

When the first node that finds the correct solution to the problem it broadcasts it again to the entire network. Since the correct solution is easy to check by others, the rest of the network can agree with a valid transaction and the node that solved the problem first is rewarded by tokens. The reward can be either a transaction fee or fully new tokens, when the mining process is also used as a way to issue more money for circulation.

An important feature of mining is that it should be incentivized in a way that makes the nodes willing to spend their computing power to solve the cryptographic hash functions. This means that the reward should exceed the cost of the used power. In principle, the nodes could also use their computing power to find solutions to fake transactions in order to double-spend their tokens, for example. Because of this, the system should be incentivized so that it would require unreasonably high amount of computing power to rewrite all the previous blocks to tamper the ledger. It would therefore be more attractive to validate the real transactions and be rewarded according to the rules. Böhme et al. (2015) state that "the probability of an entry becoming superseded goes down as more blocks are built on top of it, eventually becoming very low." This is due to the fact that in order to tamper the history of transactions, e.g. to claim owning of an untrue amount digital money, all previous blocks should be rewritten because all transactions have to refer to preceding transactions.

Even though proof-of-work consensus protocol is viable in establishing scarcity and prevent double-spending, it does not come without problems. The main issues are related to its energy-intensity, costs and scalability. For example, Becker et al. (2013) estimates that if proof-of-work was used as a mechanism to authenticate all electronic payments in the world, it would impose an ecological footprint similar to global commercial air traffic. O'Dwyer and Malone (2014)

have shown that the energy consumption of bitcoin mining is comparable to the electricity consumption of Ireland.

Croman et al. (2016) argues that the increasing popularity of blockchain-based cryptocurrencies has made scalability a primary and urgent concern. Thereby, the need for finding faster, more scalable and more energy-efficient consensus algorithms is important.

Proof-of-Stake

Instead of mining with computational power, as in the proof-of-work protocol, in the proof-of-stake (PoS) protocol the mining is done by using the tokens which an agent owns within the system. In PoS, a miner is putting up a stake, or is locking an amount of coins, to verify which copy of the ledger is correct. According to Bentov et al. (2016), "the rationale behind proof-of-stake is that entities who hold stake in the system are well-suited to maintain its security, since their stake will diminish in value when the security of the system erodes". Proof-of-stake serves as a backbone for cryptocurrencies like peercoin, blackcoin and NXT, for example.

Bentov et al. (2016) identifies at least two major issues related to pure proof-of-stake systems. First, the initial distribution of tokens might give disproportionately huge power to first movers since they own a large proportion of the tokens, which are used to decide which copy of the ledger is correct. Second, the network is fragile due to a problem called "nothing-at-stake". If there is no risk of losing tokens in the protocol (alike spending computing power in the PoW) it might be beneficial to vote purposefully for a wrong copy or simultaneously vote for multiple copies, in order to double-spend tokens, for example. Thereby, the tokens should be made scarce artificially by coding the scarcity to the algorithm of the blockchain network and simultaneously making sure that placing a stake to vote for the correct copy of the ledger is properly incentivized.

Alternative Protocols

Developers and researchers are working also on alternative ways to manufacture distributed consensus since PoW and PoS have both their own limitations. According to Croman et al. (2016), the possible alternatives include:

- Hybrids of proof-of-work and proof-of-stake

- Consortium consensus, where critical protocols are executed by small sets of trusted entities
- Sharding, where task of consensus is split among concurrently operating sets of actors
- Proof-of-validation, implying a security deposit of voters
- Proof-of-capacity, taking advantage of free storage capacity in voting
- Proof-of-importance, where the voting power depends on peer reputation

3.2 Example: Bitcoin Blockchain

Bitcoin gives a good example of the use of the proof-of-work protocol. "Peer-miners", who can be anyone in the bitcoin network, maintain bitcoin by adding new information to the ledger. Peer-miners solve cryptographic hash functions iteratively using computing power. Participating to the mining process is voluntary, but when new information is added to the ledger peer-miners are favoured with new bitcoins and therefore incentivised to maintain the ledger in a fully decentralized way.

When new information (a block) is added to the chain of previous transactions, other nodes of the network need to accept that the solution to the hash function is correct, implying that the new transaction is valid. According to Nakamoto (2008), the six main steps to run the bitcoin network are the following:

1. Transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block (decrypts the hash function).
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Once the new transactions are accepted, the ledger cannot be changed without redoing all of the work required to find the proof-of-work solution at the first place. For example, if a node is claiming to own assets that it actually does not own, it should redo all the work done to create a transaction history in which the balances would show that the dishonest node has the assets. In addition, the node needs to get the acceptance of other nodes for changing the transaction history. In practice, this means that the system is secure as long as honest miners collectively control more of the network's computing power than any cooperating group of attackers. As the number of nodes in the network grows, the possibility of cooperating attackers is likely to become lower.

4 Monetary-Centered Approach

In this chapter, blockchain is reviewed from the monetary point of view, first by reviewing how digital money and cryptocurrencies could potentially serve as a store of value, a medium of exchange and an unit of value. Second, the features of cryptocurrencies are studied through the quantity theory of money. Third, the possible implications and opportunities of digital money on monetary policy are discussed.

4.1 Properties of Blockchain Cryptocurrencies

Money facilitates exchange by allocating resources efficiently and measuring value of various goods and services. Usually money we refers to central bank issued fiat currencies. However, this is not self-evident. Whereas historically currencies were chosen from among existing commodities, modern technology (including blockchain) gives unprecedented flexibility in designing the attributes of currencies (Gans and Halaburda, 2015a).

4.1.1 Currency Definitions

Fiat currency: "Any legal tender designated and issued by a central authority that people are willing to accept in exchange for goods and services because it is backed by regulation, and because they trust this central authority."(ECB, 2012)

Digital money: "A digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically." (ECB, 2012)

Cryptocurrency: A decentralized digital currency, which does not need financial intermediaries in order to perform electronic transactions. It has neither a central bank nor other authority in control of its monetary policy. (Peters et al., 2015)

Thus, two types of digital currencies exist: cryptocurrencies and non-cryptocurrencies (Dandapani and Dandapani, 2017). Cryptocurrencies are decentralized peer-to-peer digital currencies based on computer cryptography (e.g. blockchain). Popular cryptocurrencies include bitcoin, litecoin, zerocoin and peercoin. In turn, examples of digital non-cryptocurrencies include Facebook credits, Microsoft

points and Amazon coin, which are backed by the named corporations and are thus not decentralized by definition.

4.1.2 Functions of Money

Any kind of money must fulfill three basic functions: unit of account, medium of exchange and store of value (Jevons, 1885). Unit of account means that the value of goods can be assessed in terms of a uniform intermediary. Medium of exchange means that money is an intermediary used for transactions, and thus economic agents do not need to engage in barter exchange. Money must also be able to transfer purchasing power to some future date and therefore serve as a store of value.

According to Böhme et al. (2015), Peters et al. (2015), Ali et al. (2014) and Bank bankofcanada.ca (2014), bitcoin fulfils these three basic functions to some extent, but not in the way that fiat currencies do. Next, the three functions of money are discussed in the context of cryptocurrencies.

Cryptocurrencies as a Store of Value

The parties of a transaction should always consider - at least temporarily - an asset as a store of value in order to fulfil, even theoretically, the other two basic functions. Thus, an asset should have an expectation of positive value also in a future date, which basically is a result of sufficient demand and supply of the asset. Next, the possible sources of demand and procedures of supply of cryptocurrencies are reviewed.

Demand

According to Dwyer (2015), foreign currency exchanges are probably the most obvious way in which the use of cryptocurrencies can become widespread. Dwyer (2015) observes that if a person holds accounts in various currencies, it is cheaper to transfer funds from one account to another through a cryptocurrency compared to the current cost of obtaining foreign currencies via exchange. Also for this reason using cryptocurrencies for international remittances are a possible source of demand (Böhme et al., 2015).

Another important feature of cryptocurrencies is their perceived anonymity. According to Catalini and Gans (2016), illegal marketplaces were one of the early ones to use bitcoin and thus bootstrapped its value. Many publications,

including Athey et al. (2016), Raskin and Yermack (2016) and Peters et al. (2015) have documented this source of demand.

The good portability properties of digital money in general (not only cryptocurrencies) implies lower transaction costs in transferring big amounts of value. Correspondingly, the ease to divide and recombine digital money make practically any denomination possible. This also provides a technical infrastructure for different applications like micropayments. (Peters and Panayi, 2016)

Cryptocurrencies are also an attractive store of value in countries with high financial instability. They may provide security especially in countries with high national debt (Gans and Halaburda, 2015a), and protection against the risk of inflation. For example, Moreno (2016) finds that in Argentina the demand for the cryptocurrency bitcoin has increased during periods of high inflation. Cryptocurrencies are also an appealing alternative in countries facing currency devaluation or where trust in the government is low (Catalini and Gans, 2016). In addition, events such as India's demonetization of the 500 and 1000 rupee notes can increase consumers' interest in cryptocurrencies (Catalini and Gans, 2016).

To summarize, foreign exchanges, international remittances, online marketplaces, financial crises and other instabilities are the identified reasons why of cryptocurrencies and alternative payment mechanisms may increase their popularity.

Supply

In order to have a positive value, the supply of money should be scarce. In the case of cryptocurrencies, scarcity is usually pre-determined and coded in the algorithm. For example, bitcoin's nominal quantity of money is an increasing concave geometric series (figure 3) until the total number of coins in circulation reaches the upper limit of about 21 million in 2041 (Nakamoto, 2008). In turn, cryptocurrency litecoin has ex-ante determined its annual supply up to 84 million coins (four times more than bitcoin) by 2140 (Litecoin.org, 2017).

In fact, money supply is likely to turn even negative in the end of the mining period. Bitcoins are constantly irreversibly destroyed as users forget their private keys or coins are sent to accounts that are not in use anymore. In ad-

dition, if an owner dies and their private key is not accessible, their tokens are taken out of circulation.

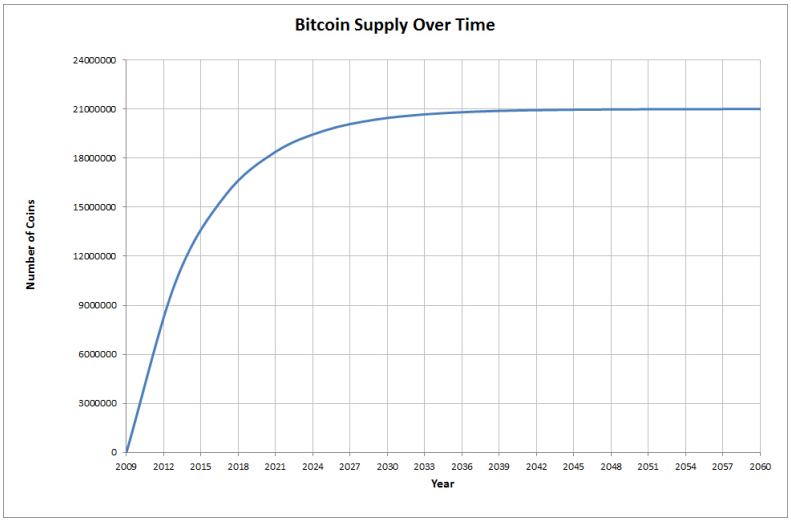

Figure 3: Bitcoin Supply over Time

Besides scarcity, there are other issues related to the supply of cryptocurrencies: How are decentralized cryptocurrencies created? If there is revenue from creating the currency, who receives it? What issues determine changes in the nominal quantity of money? (Dwyer, 2015)Both networks, bitcoin and litecoin, exploit the idea of mining, where money supply is channelled through peer-miners who are rewarded for using computing power to validate transactions and thus keeping the network running.

Digital currencies give unprecedented flexibility to design different attributes to currencies (Böhme et al., 2015). Cryptocurrencies are usually based on an open source software, this creates an opportunity for anyone to access the original blockchain code to learn, copy and design their own money (Kane 2017). This creates an exceptional potential for experimentation of different properties of money (Gans and Halaburda, 2015b).

Cryptocurrenices as a Medium of Exchange

If assumed that a cryptocurrency fulfills the fundamental preconditions of positive value, i.e. sufficient demand and supply, what would then be the qualities of a good medium of exchange? According to Kiyotaki and Wright (1989) a critical factor is whether economic agents believe that a cryptocurrency can serve as a medium of exchange. This refers to the scope of the acceptance of the currency.

Therefore, at least the regulatory environment and the recognition of major marketplaces are important factors in making the currency a good medium of exchange.

The website Spendbitcoins.com (2017) listed over 100 000 large and small merchants who accept bitcoins. Some significant brands like Amazon, the travel agency Expedia and the fashion store Asos were included in the list. Still, the universal acceptability of bitcoin has been slow and the currency has suffered on volatility issues (Dandapani and Dandapani, 2017). The regulatory environment has an important role in the acceptance of bitcoin. The legal treatment of bitcoin varies widely across countries, ranging from Denmark, where cryptocurrencies are not regulated at all, to Thailand where using bitcoins has been criminalized (loc.gov, 2014).

According to Holdsworth (1914), in addition to acceptance other qualities of a good medium of exchange include divisibility, portability and existence in sufficiently large quantities. As explained earlier, divisibility and portability are advantages of digital money relative to fiat money (Barber et al., 2012; Peters and Panayi, 2016). The sufficiently large existence means in this case the supply of the digital money, which depends on the chosen design principles. The technology gives flexibility in designing and experimenting different attributes. However, cryptocurrencies, which are based on the proof-of-work consensus mechanism like bitcoin, might face obstacles related to scalability when the money in the circulation increases. According to Böhme et al. (2015), if bitcoin expanded to include a huge volume of transactions, the storage burden would need to be addressed. Furthermore, updating the proof-of-work blockchain entails undesirable delays, making bitcoin too slow for many in-person retail payments. This would also consume high amounts of energy. Thereby, whereas cryptocurrencies based on proof-of-work create scarcity and security, they also have some undesirable technical properties limiting their scale and ability to serve as large scale media of exchange.

4.2 Cryptocurrencies and Quantity Theory of Money

The quantity theory of money builds a link between the nominal money supply, price level and size of the real economy (Friedman, 1968). Traditionally, monetary policy aims to slowly increasing prices with stable growth of economy.According to the theory, in a closed economy price level (P) times real value of transactions (T) equals money output (M) times money velocity (V).

$$P * T = M * V \tag{1}$$

In the context of cryptocurrencies, the real transaction value (T) is equivalent to the extent of economic activity using the underlying cryptocurrency. Velocity (V) refers to how fast money passes from one holder to the next. Money supply (M) on the underlying issuance model which differs from one cryptocurrency to another as explained earlier. In order to study the price level as a dependent variable, from equation (1) can be derived:

$$P = \frac{M * V}{T} \tag{2}$$

Increase in money supply (M) or velocity (V) imply higher prices if other factors are held constant. Higher real transaction volume (T) would in turn cause downward pressure on prices. Following this, an interpretation can be made that given a constant velocity (V) and an increase in real transaction volume (T), in the case of the money supply (M) turning negative, a downward pressure on prices follows. Böhme et al. (2015) points out thereby a question "what happens when the size of an economy grows at a different rate than the quantity of money in that economy?" A declining price level is usually associated with money hoarding and the postponement of spending, which can lead to a vicious deflationary circle.

However, a fair assumption is that in the near future, prices will be denominated in national fiat currencies. Thus, the role of cryptocurrencies would be to serve as a store of value and as an alternative payment method for some transactions. Thereby, the deflationary features of a cryptocurrency would not mean a decline in the prices at the economy level but rather a possible increase in the value of the underlying cryptocurrency.

If there was downward pressure on prices (equation 2) due to the declining money supply (M) and increase in real transaction volumes (T), there would also be pressure for the higher value of the cryptocurrency in question. A lower price level (P) would mean lower cryptocurrency-denominated prices, but the exchange value of the cryptocurrency would actually be higher if a fiat currency is still the primary unit of account. In this case, the underlying cryptocurrency would have higher purchasing power in a future date and the pressure of increase in its value would make the cryptocurrency more attractive as a store of value.

The conclusion is that if the supply is fixed and decreasing, or even negative,

there should be some sources of demand for cryptocurrencies in order to store healthy value as a medium of exchange. Otherwise the value would be purely speculative. As identified in the previous section, the possible sources of demand include foreign currency exchanges, international remittances, anonymous marketplaces, and marketplaces where the portability of value and divisibility are important.

4.3 Blockchain and Monetary Policy

The general understanding is that monetary policy would be hard to implement without an increasing money supply. If this is true, it is not likely that cryptocurrencies with fixed or declining money supply would gain ground as a mainstream medium of exchange or a unit of account. However, they might still become a mainstream store of value (Böhme et al., 2015).

Central banks could still apply the blockchain technologies to develop their monetary policies. For example, blockchain technologies could enable central banks to directly provide citizens with digital, central bank money (Catalini and Gans, 2016). This is an interesting feature to implement different basic income models, for example, or to providing quantitative easing directly to citizens. In addition, blockchain can provide a technical infrastructure to manage money supply and interest rates more effectively. (Catalini and Gans, 2016)

Roberds (2016) argues that the emergence of digital currencies is analogous to the emergence of banknotes in England in the 17th century. First, the demand for cash is declining, but second, cash is also an enormous source of revenue for central banks and government beneficiaries and a robust channel for central bank financing. Roberds (2016) predicts that for these reasons at some point in the not-too-distant future the "business model" of central banks and the architecture of money may need remodelling. He also argues that "we should not be surprised to see new payment technologies dominated by a very few players, of a size sufficient (e.g. Google) to internalize the relevant network effects."

5 Innovation-Centered Approach

Blockchain is an ICT innovation, which enhances the productivity of several processes but also creates new marketplaces through the reduction of transaction costs. This is primarily a consequence of the decline in 1) the cost of verification, and 2) the cost of networking (Catalini and Gans, 2016). However, the mainstream adoption of blockchain, which would unlock the benefits of interoperability and the network effects[6] of the technology, requires significant diffusion process. In order for this to happen, there should be actors who are interested to invest in the technology.

Technological change can be either exogenous, where the change is external to the economic system, or endogenous, which is driven by intentional investments by profit-maximizing agents (Romer, 1990). Endogenous change requires naturally the expectation of positive returns to investments. This means that the technology should generate savings through efficiency, or it should bring new sources of revenue from new marketplaces.

The process is complex from a single entrepreneurial viewpoint. Like the case is with all new technologies, blockchain entrepreneurs must take risks and gather distributed non-price information as inputs into their economic calculations over potential profitable opportunities, which often involve a lengthy period of trial-and-error experimentation (Allen, 2016). It is important to note that the inability of a single firm to appropriate all the benefits generated by the technology may result in underinvestment (Catalini and Gans, 2016).

In this chapter, the two approaches to technological change, exogenous and endogenous, are reviewed and the possible sources of productivity increases gained from blockchain are discussed. After that, blockchain is compared to the definition of the general-purpose technologies, which are pervasive technologies that Bresnahan and Trajtenberg (1995) argue to be the ultimate sources of long-run economic growth.

5.1 Two Approaches to Technological Change

The Cobb-Douglas production function states that the aggregate economy produces change in output (Y) as a function of change in productivity (A), change

[6] When a network effect is present, the value of a product or service increase as a function of the number of others using it (Metcalfe's law)

in capital (K), and change in labour (L).

$$Y = AK^{\beta}L^{\alpha}$$

In the advanced economies, the increase in productivity is considered generally as the most important driver of long-term growth. Economists widely agree that technological change is the single most important driver of productivity growth. However, models differ whether technological change is a consequence of endogenous or exogenous factors to the economy. The Solow-Swan growth model (Solow, 1956; Swan, 1956) assumes that long-run growth is achievable only through exogenous technological change, which is unexplained within the model. In turn, the modern growth theory (Romer, 1986; Lucas, 1988) explains long-term growth through endogenous forces like investment in innovation and education, which also leads to technological change and more efficient labor and capital.

5.1.1 Blockchain and Technological Change

In the endogenous technological change, the productivity increase is a result of purposeful investment to the research and development. As the maximization of profits is a powerful driver of technological change (Huesemann and Huesemann, 2011), if the expected profits are positive, the investments occur that drive the technological change.

According to Catalini and Gans (2016), usually a single firm that invests in a new technology is unable to appropriate all its benefits. This in turn can cause underinvestment in the technology and suboptimal outcome and public support is needed to correct the market failure. The technology "will only be developed if a firm is able to appropriate its benefits through complementary assets, or if a public effort supports its early development as in the case of the internet" (Catalini and Gans, 2016). Without any external influences, technological change is a social process which can be strongly biased by a short-term financial interest (Huesemann and Huesemann, 2011). Thereby, the diffusion of any new technology is likely a result of both, exogenous and endogenous factors.

In 2016, the value of investments in blockchain initiatives exceeded 1 billion USD (Johnson, 2016). However, according to Zhao et al. (2016), "business research in blockchain is found mainly in the conceptual level that conceptualizes blockchain innovations in business and in the prescriptive level that outlines business applications of blockchain". The real business potential and thereby

the premises for the endogenous technological change of blockchain are not yet especially clear.

Also consultants, such as Gartner (2016), expect that overinvestment to the blockchain technology has occurred and blockchain is going to face a "peak of inflated expectations" (see figure 4).

Figure 4: Gartner Hype Cycle for Emerging Technologies, 2016

The prescriptive sources of blockchain-enabled business models can be divided into two categories: cost savings through efficiency improvements and increased revenue through new marketplaces. Next, these two categories are reviewed.

5.1.2 Blockchain-Enabled Efficiency Improvements

In general, an innovation that enhances productivity enables more to be done with less. Yet how is this gain possible in the context of blockchain? According to Davidson et al. (2016b), it is not that the electrons now move faster, or that the processing engines are more efficient (metaphorically). Instead, the source of the productivity gain can often be traced to an organizational efficiency gain. Blockchain decrease production costs by changing the organizational form by which value is created, often stripping out layers of activity that are no longer needed.

Different processes of transactions, in for example online commerce and in-

vesting, require verification of ownerships, checks and balances. According to Catalini and Gans (2016), blockchain decreases the cost of verification and thus improves the efficiency of these transactions. Also Davidson et al. (2016b) claim that decentralized solutions to ledgers can become increasingly cost efficient compared to centralized solutions, leading to the described efficiency gain.

According to Zhao et al. (2016), financial sector is the leader in blockchain-related business innovations (Zhao et al., 2016). Peters and Panayi (2016) suggest that blockchain may enable efficiency improvements in the banking sector at least in:

- Back-end bookkeeping systems, i.e. banking ledgers;
- Transaction processing systems;
- Trading and sales functions;
- Interbank money transfer systems;
- Settlements of financial assets.

Other possible blockchain-enabled efficiency improvements are related to for example supply chain management (Pilkington, 2015), stock exchange (listing, trading, voting, ownership transfers and more accurate records) (Yermack, 2017) and corporate governance (providing data efficiently for investors, auditors and other stakeholder groups) (Kim and Laskowski 2016, Yermack 2017).

Even though some sources of efficiency improvements can be identified, Zhao et al. (2016) and Peters and Panayi (2016) point out that they are unaware of research that would explain in detail exactly how and in what form blockchain technology could provide these benefits. Thereby, the exact source and dynamics of these cost savings remains unclear and, as Zhao et al. (2016) put it, "research in the descriptive level is lagging".

5.1.3 Blockchain-Enabled New Marketplaces

Another source of possible entrepreneurial profits and thus endogenous technological change is the emergence of new marketplaces. This means that profits rise when technology facilitates the exchange of items and services whose exchange was not previously efficient or relevant.

According to Catalini and Gans (2016), blockchain allows market participants to

perform costless verification, and thereby it lowers the costs of auditing transaction information. Thus it makes it efficient to make transactions in the marketplaces where it would previously have been inefficient due to low the transaction value compared to the transaction costs. An example of this are different sharing economy platforms that require a verification of trust and mechanisms to monitor reputation and payment systems. If on top of that the transaction values are low, creating a profitable business model is challenging to create.

New markets can emerge in the banking sector as well. The development of a more interoperable financial platform through blockchain could substantially lower the entry costs for new players in these heavily regulated markets (Catalini and Gans, 2016). This could provoke investments in startups that try to challenge existing business models.

Another concrete examples of a new marketplace is the emergence of digital currencies. For example, bitcoin has not created just a new representation of value but also completely new industries, including bitcoin mining companies, wallets and exchanges, which have attracted investments and driven the technological change.

An interesting feature of especially cryptocurrencies is that cryptocurrency protocols can incentivize the emergence of networks of exchange through native cryptocurrency tokens (Catalini and Gans, 2016). According to Catalini and Gans (2016), "relative to open source projects, which have to rely on donations of time and resources, ... cryptocurrency protocols can offer direct, monetary incentives to fund their growth." In the end of chapter 6 is an example how a decentralized cooperation can be incentivized to grow.

5.2 Blockchain as a New General-Purpose Technology

Bresnahan and Trajtenberg (1995) have suggested that "general-purpose technologies" (GPTs) are the ultimate sources of productivity increase, and thus also of the long-run economic growth. Most of GPTs play the role of "enabling technologies", opening new opportunities rather than final solutions (Bresnahan and Trajtenberg, 1995). Traditional examples of GPTs are the steam engine, the electric motor, semiconductors and the internet.

By definition, GPTs are technologies that are pervasive (spreading to many sectors), have inherent potential for technical improvements (improving over time)

and innovational complementarities (spawning new innovations). With these qualities, GPTs generate economic activity and eventually generalized productivity gains. They are pervasive technologies that shape societies and cultures and lead to monumental changes in economic organizations. (Bresnahan and Trajtenberg, 1995).

For example, according to Catalini and Gans (2016) and Allen (2016), blockchain has the potential to become a new general-purpose technology. Next, the three features of GPTs, and the potential of blockchain to become one in the future, are analyzed.

5.2.1 Pervasiveness of Blockchain

Blockchain is used across different sectors. The pervasiveness reaches anywhere where a protocol for sending, receiving, confirming and recording value or information is plausible and clear identification by one or more actors in the network is possible (Pilkington, 2015; Crosby et al., 2016). According to for example Kane (2017) and Allen (2016), the blockchain technology is applicable to a wide variety of sectors and has the potential to expand rapidly and is thereby a pervasive technology.

Examples of applications sectors of blockchain vary from digital identity providers (e.g. OneName and BitID) and anything where the ownership and transaction history of assets is important (ownership rights, real estate, automobiles, physical assets) to insurances and voting-systems (e.g. Bitnation and Bitcongress). Swan (2015) argues that many new and different kinds of governance models and services might be possible using blockchain technology. According to Swan (2015), blockchain could become both "the mechanism for governing in the present, and the repository of all of a society's documents, records, and history for use in the future - a society's universal record-keeping system."

5.2.2 Potential for Technical Improvements of Blockchain

GPTs are technologies that are capable for further improvement and change (Carlaw and Lipsey, 2006). Blockchain's form as an open source software gives it great potential for technical improvements over time. According to Kane (2017), the power of open source software lies in the opportunity for anyone to access the original blockchain code to learn, copy and create their own applications. For example, from the launch of bitcoin, people have taken its open source code and developed their own unique applications. According to the

survey by Kane (2017) with over 200 blockchain companies, "in the relatively short time that blockchain technology has existed it has changed innumerable times as people experiment and tinker with it trying to find new and more useful applications."

As noted in chapter 3, different consensus protocols for blockchain are continuously developed (Croman et al., 2016). In addition, the supporting innovations in processing, storing and shipping of information are creating room for more efficient blockchain technology.

5.2.3 Innovational Complementarities of Blockchain

According to Allen (2016), blockchain is complementary with existing technologies, institutions and organisations (e.g. banks), including 'economies' such as the physical parts of the sharing economy and the internet of things (IoT).

The blockchain application platform Ethereum states that the potential value of blockchain lies in its interoperability and the exponential value that comes from creating networks (Buterin, 2014). Improvement in one area makes subsequent improvements in other areas increasingly beneficial. Allen (2016) explains that blockchain "creates new ways to create" and Kane (2017) argues that blockchain provokes further innovations through for example more efficient crowdfunding and crowdsourcing technologies.

5.2.4 Is Blockchain a New GPT?

Altogether, technological change and the emergence and mass-adoption of a new GPTs is likely a combination of external and endogenous forces. Like explained earlier, blockchain has already shown its pervasiveness in different sectors and applicability in different functions. It is also complementary with for example banking, IoT and the sharing economy (Allen, 2016). Blockchain itself has room for technical improvements. This is powered by open source software development, progress in more efficient consensus mechanisms and potential continuation of increase in the processing capacity. These features makes it a potential GPT in the future.

6 Governance-Centered Approach

The governance-centered approach to the economics of blockchain studies whether blockchain could be an institutional technology for coordinating the economic actions of people and organisations. Herein governance is defined as "proofs of interaction and decision-making among the actors involved in a collective problem" (Hufty, 2011).

Markets and firms are alternative institutions for economic governance (Williamson, 1975). The basic insight of new institutional economics is that the transactions that occur in markets create room for opportunism. Firms and intermediating centralised actors like banks, have emerged to mitigate this opportunism (Williamson, 1975, 1985; Coase, 1937).

In this chapter the basics of new institutional economics are reviewed, followed by an analysis and examples on how blockchain can actually facilitate more decentralised interactions and decisions. Finally, the potential of blockchain to incentivize decentralized production is explained through an example of Backfeed, which is described as "a social operating system for decentralized cooperation".

6.1 New Institutional Economics

The governance-centered approach can be analyzed through the new institutional economics. New institutional economics studies markets and firms as alternative institutions of economic governance, i.e. institutions that organise transactions. This discipline is interested in why some transactions occur in markets and some in hierarchies (firms).

Whereas the neoclassical analysis of economics focuses on production costs achieved through efficiency improvements, the new institutional economic analysis (also known as transaction cost economics) emphasizes the notion of transaction costs and the efficient use of organizations and markets. Transaction costs in markets stem from information costs, bargaining costs and enforcement costs of contracts (Coase, 1937). According to Dahlman (1979), information costs are such a costs that occur for example when economic agents spend resources to determine whether the required product is available on markets or they are looking for the best available price. Bargaining costs arise from drawing up an appropriate contract for a transaction and enforcement costs are "the costs of making sure the other party sticks to the terms of the contract" (Dahlman,

1979).

Williamson (1975, 1985) argues that opportunism arises in market exchange for several reasons. Williamson (1993) argues that trust between economic agents is "calculative". Calculative trust "raises via sober assessment of the costs and benefits to the other party of exploiting another's vulnerability" and presumes that without correct economic incentives, pure trust cannot facilitate transactions (Williamson, 1993).

According to Williamson (1985), the existence of organizational form is largely shaped by the need to control opportunism. Markets are often efficient governance institutions for spot contracts (immediate payment and delivery), but where the economic activity requires asset specificity (coordinated investment through time), frequency (ongoing relation between parties) or uncertainty (uncontractible dealings), alternative governance institutions are needed to deal with the hazard of opportunism (Williamson, 1985). Whereas opportunism occurs in transactions made in markets, hiring people would "bound [them] by some common purpose to achieve objectives" (Coase, 1937). Another form to mitigate opportunism is to introduce a trusted third party, like a bank or a real estate agent, who would facilitate the trust between the two agents of the transaction (North, 1990; Williamson, 1985).

6.1.1 Trust, Opportunism and Blockchain

According to Williamson (1993), three forms of trust exist: personal, calculative and institutional. According to Williamson (1985), personal trust cannot be a safeguard of business relationships. The institutional form of trust refers in turn to the social and organizational context within which contracts are embedded (North, 1990).

In the simple trust game example (figure 5), consider that P2 would like to pursue some income as a taxi driver but does not own a car. However, P2 can rent a car from P1 by agreeing to pay a partial return of the income from the pursued profits as a rent. If the payment is paid as agreed, both get a payoff r. Assume that P1 and P2 have only calculative trust on each other and the transaction take place in a market without a trust-facilitating intermediary. Now, if P1 decides to trust P2 and rents out the car, P2 has an incentive to defect (e.g. lie about the generated income) if the payoff is $1 > r$. If P1 is aware of this, she does not trust P2 at the first place and the potentially mutually beneficial

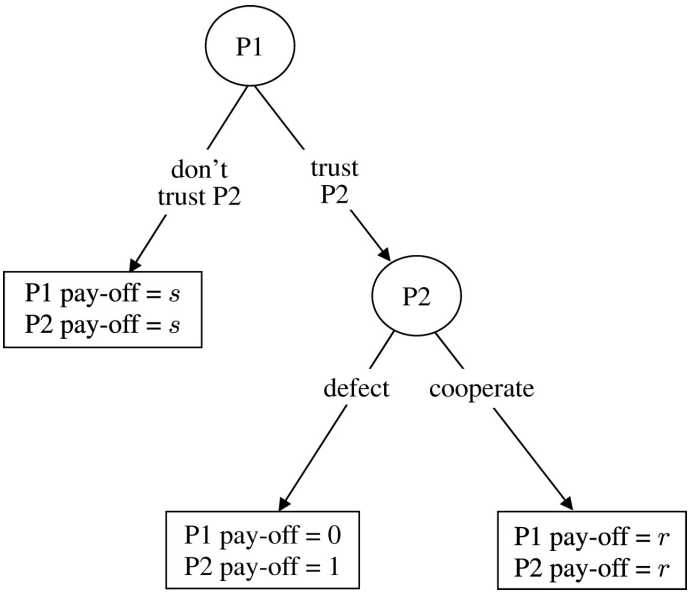

Figure 5: Simple Trust Game (Source: McNamara et al. 2009)

set of transactions does not take place at all. Thereby, due to the information asymmetry, both get an outcome s < r.

One solution to the dilemma presented above is to establish a taxi firm where a capital owner P1 hires P2, and thus bounds the incentives of the two parties to common objectives. This kind of organization could formalize sanction systems and monitor individual actions in this "internal market".

Another solution to the dilemma is to establish a neutral third party institution that punishes P2 for the defect to the extent that the payoff r for cooperation is higher than for the defect that would be 1 - p (p = punishment) (Figure 6). In the digital economy, the centralized third-party authority could be a platform provider for drivers and cars. The platform could, in the case of betrayal, prevent P2's access to the platform in the future, creating an incentive for P2 to cooperate. The punishing authority, or "enforcement agency", can also be a society at large or the risk of social ostracism (Dasgupta, 2000). For example, banks exist as third party intermediating organizations because there are substantial costs – physical costs, information costs, and coordination costs – that occur when the market is used for matching the supply and demand of financial assets (Dow and Earl, 1982). Moreover, banks are maintaining a centralized ledger of transactions and other records, and their business model consists of

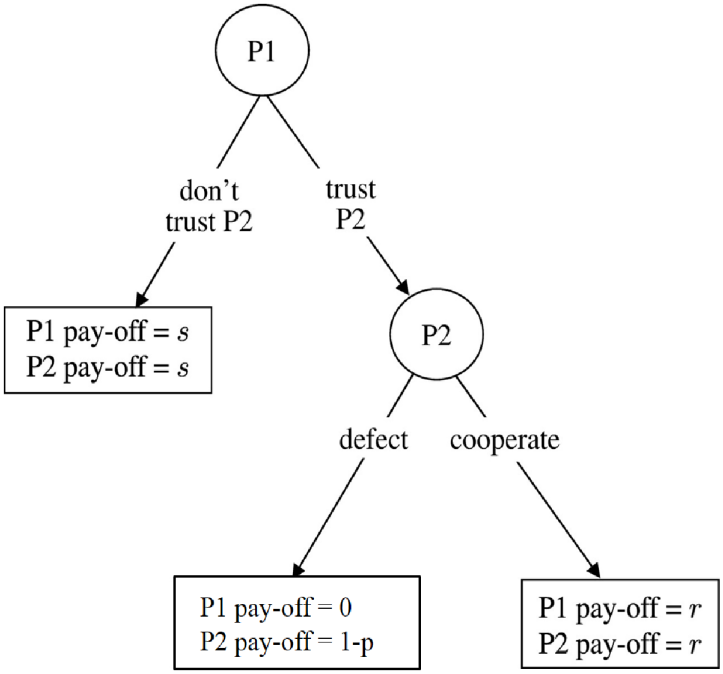

Figure 6: Simple Trust Game 2

economizing at the margin of transaction costs. Banks have created and employ a reputational incentive mechanism that enables them to enforce contracts at a lower cost than what distributed agents (i.e. public without a bank) could. This is due to the ability of banks to exclude defaulting borrowers from subsequent access to finance (MacDonald et al., 2016).

The utopian views of blockchain argue that blockchain could serve in the future such as an intermediary, or enforcement agency, and therefore it will disrupt every market by eliminating the need for intermediation by facilitating trust. More realistically, Catalini and Gans (2016) argue that blockchain is "more likely to change the scope of intermediation" through reduction of transaction costs and by allowing the formulation of new types of marketplaces.

6.2 From Hierarchies and Intermediaries to Markets

Via the bitcoin network, blockchain has proved to be able to disseminate trust over a network of unknown agents and thereby let people who have no particular confidence in each other to collaborate without having to go through a neutral

central authority. But how does blockchain facilitate trust and eliminate opportunism? According to Swanson (2014), this is made possible with public transparency of previous actions (constituting to the reputation of the actors) coupled with the consensus protocol, and smart contracts that are executed automatically.

6.2.1 Public Reputation and Consensus Protocol

If P1 and P2 play this (figure 5 and figure 6) one stage game infinitely, and the future is important enough, an equilibrium exists where P2 has an incentive to cooperate and P1 to trust P2. Thereby, reputation becomes an important incentive mechanism that facilitates trust in anonymous online markets (Tadelis, 2016).

If the reputation follows an actor, the game would keep going infinitely from the viewpoint of P2. In the taxi driver example, in the case of indefinite game, if P2 is interested in pursuing an income as a taxi driver, he can expose his aggregated reputation accumulated from several other platforms to P1. Thereby, P1 would more likely trust P2 and rent a car with good conditions. Moreover, if both actors know that their counterparts' reputation follows them to other platforms automatically, they also know that continuous cooperation implies higher sum of future payoffs for both.

$$(r_1 + ... + r_n) > 1$$

Since a principle of calculative trust is that trust is based on a "sober assessment of the costs and benefits to cooperate or exploit trust" (Williamson, 1985), as learned earlier, P1 can assume that P2 has an incentive to cooperate. Thus, a cooperative equilibrium exists and mutually beneficial interaction is likely to be initiated.

Meta-Reputation and Blockchain

Public reputation systems already provide premises for numerous online peer-to-peer marketplaces, like Amazon, eBay, Uber and Airbnb. However, the firms govern these reputations systems centrally. In addition, the reputation in one platform does not follow an actor to other online platforms.

If some sort of meta-reputation system, which leverages the reputation from one platform to another, would be governed by a centralized intermediary, verifiability and privacy could become a problem (Tadelis, 2016). According to

Tadelis (2016), blockchain may provide solutions, which would make the online platforms work more decentralized and efficiently.

Bitcoin has demonstrated in the financial context that blockchain, i.e. auditable computing is possible using a decentralized network of peers accompanied by a public ledger (Zyskind et al., 2015). According to Tadelis (2016), analogously, the blockchain technology can be used in creating a secure and robust decentralized reputation system. In this case, the gatekeeper of the data are people themselves. According to Catalini and Gans (2016), blockchain could improve the data protection and create an economy, where people would be able to license out subsets of personal information and to revoke access when necessary and not be reused in the future outside of the original transaction.

Similarly, as banks employ reputational incentive mechanisms by being able to exclude defaulting borrowers from subsequent access to finance, the same result could be achieved through decentralized reputation systems. In this case, other peers in the network can exclude the defaulting borrower from subsequent peer-to-peer loans. The advantage of the blockchain technology is that the public-private cryptography enables simultaneous reliable verification of transactions but also a sufficient degree of privacy. In practice, an agent with a good payment history can leverage the reputation and get access to a platform with good conditions. However, any single centralized intermediary would not be able to gather, own and possibly exploit the personal information for other purposes without consent of the customer.

This implies that the technology enables establishing and maintaining markets for reputation, where customers retain greater control over their data and firms can dynamically bid for access. In addition, meta-reputation can be used to address information asymmetries and other market failures as well as monitor market participants at a substantially lower cost. (Catalini and Gans, 2016)

6.2.2 Automatic Execution with Smart Contracts

Blockchain-based smart contracts are contracts that are executed automatically and are supervised by the consensus of the decentralized blockchain network. Smart contracts facilitate, verify, or enforce the negotiation or performance of a contract (Allen, 2016; Davidson et al., 2016a). According to Davidson et al. (2016b), blockchain-enabled smart contracts can increase economic efficiency problems by decreasing the information asymmetries like adverse selection and

moral hazard. In addition, they argue that smart contracts could be effective ways to load significant numbers of low probability state-contingencies into contracts, like open source libraries.

In third taxi driver scenario (figure 7), the payments from P2 to P1 are self-executed through a smart contract, which is enabled by a digital payment infrastructure and blockchain technology. If P2 fails to execute the agreed payment to the car owner, the control right of the car could automatically be transferred to P1 if the car is in the network. P1 could for example shut the car automatically down, if she is willing to do so. Thereby, P2's pay-off from defect would be s ($s < 1$), if the driving would end immediately after failing the first payment. If the reputation would follow to other platforms as well, this makes the defect

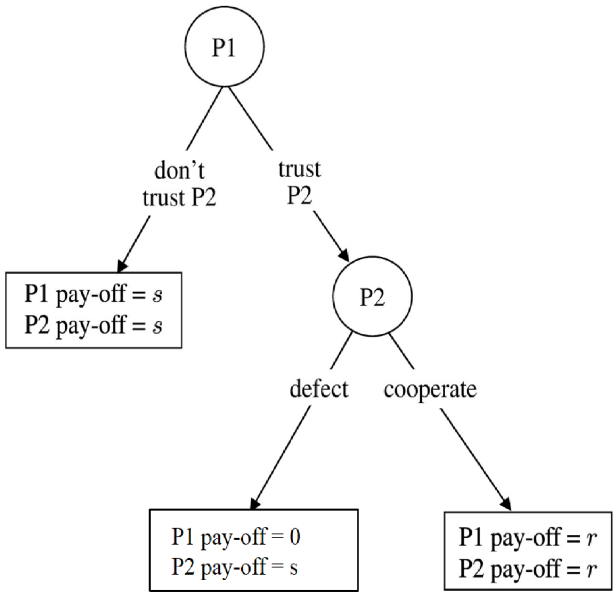

Figure 7: Simple Trust Game 3

drastically less attractive for P2 compared to the one-time single transaction. If P1 knows this, the mutually beneficial interaction is likely initiated.

Altogether, the combination of self-executing smart contracts with open reputation systems and the blockchain consensus protocols would be a powerful combination to facilitate trust among previously unknown agents. The taxi-driver example can be applied to any transaction, where recording value or information is plausible and clear identification by one or more actors in the

network is possible (Pilkington, 2015; Crosby et al., 2016).

6.3 Decline of Transaction Costs

Blockchain can mitigate opportunism, decrease transaction costs and the cost of verification (Catalini and Gans, 2016; Davidson et al., 2016a). Moreover, according Davidson et al. (2016b), the transaction costs can potentially decrease through smart contract architecture, which would decrease the costs of writing and enforcing contracts.

The basic insight that new institutional economics can bring to the economics of blockchain is that blockchain can facilitate a shift from firms towards markets, as well as decrease need for trusted intermediaries (Davidson et al., 2016a,b). According to Evans (2014), blockchain can be instrumental in "reinventing and rebuilding modern economies and societies something closer to a peer-to-peer platform". This means enabling the basic necessary order of production, exchange and coordination to take place with smaller contributions from large central controlled organizations (Davidson et al., 2016a,b).

According to Davidson et al. (2016b), if the model of Williamson (1975) of firms and markets is correct and effective cooperative economic activity and investments are stymied by opportunism, blockchain will be a revolutionary institutional innovation. In this case, more transactions can take place without intermediaries (Davidson et al., 2016a). Moreover, according to Catalini and Gans (2016), if assets are fully digital and ownership over them is not exclusive to a trusted intermediaries, new business models can emerge since new entrants can compete for the same market at a lower cost.

This would imply a shift towards a more decentralized economy (Evans, 2014). However, it is unlikely that intermediaries would altogether disappear from transactions but the way they are adding value might change (Catalini and Gans, 2016).

6.4 Blockchain and Decentralized Cooperation

Shareable goods, services and actions have high use value but low exchange value, which poses challenges to the market price system (Pazaitis et al., 2017). The dilemma becomes more significant in the knowledge economy: data is not scarce in the same way that physical resources and it actually thrives rather

than depletes when it is used. Thereby, the logic of the data economy is different compared to industrial economy. For example, the monetary reward for writing a Wikipedia contribution is zero but the use value likely positive.

According to Pazaitis et al. (2017), the blockchain technology is enabling a new system of value, bringing economies closer to commons-oriented ecosystems. In this approach, the technology would enable new means to measure and transfer value more easily through a decentralized network.

6.4.1 Example: Backfeed and Decentralized Cooperation

Davidson et al. (2016a,b) and Pazaitis et al. (2017) are using Backfeed, a social operating systems for decentralized cooperation, as an example how blockchain enabled distributed value creation could work.

In the Backfeed model, contributors are rewarded with both liquid digital tokens and reputation representing the value of contributions. The digital tokens also represent the equity share of the organisation and can be transferred or exchanged to any other token of value. The reputation, however, cannot be transferred. Thereby, the tokens represent a liquid unit of value, in parallel with the non-transferrable reputation that represents meritocratic decision-power in the community. Blockchain enables the procedure to be fully decentralized without a central authority overlooking or deciding the value of the contributions. This is especially relevant for the sharing economy, which mostly relies on a centralised crowd-sourcing model, where people contribute to a platform but do not actually benefit from its success. (Pazaitis et al., 2017)

Next, an example of a "Decentralized cooperation" (DC) is explained through a four-stage procedure and figure 8 (Pazaitis et al., 2017):

1. An initial group of risk-taking individuals invest work and resources to the DC to accumulate tokens, which represent the equity share in the DC. At this point, the value of the tokens is purely speculative and depends on the expected value of the products or services that the DC provides.

2. As the DC starts offering a certain product or service, the tokens can be spent to the products and services. People can collect tokens either by contributing directly to the DC operations or by purchasing them from current token holders.

3. As the scale increases, the DC can start selling tokens to markets and the

DC tokens eventually become redeemable in change of a specific amount of fiat currency or other digital tokens. Over time, a dynamic exchange rate is established amongst different types of tokens, which could lead to the formation of a multilateral market of the DC tokens.

4. A price cap for the tokens is established to eliminate volatility. For instance, if the DC has accumulated 1000 USD (over the course of contributions) and issued 10.000 tokens, each token earned from the contributions will be redeemable for a value of 0.1 USD regardless of whether the market price is higher or lower. If the market price is higher, people exchange their tokens on the market rather than redeeming them. On the contrary, if the market value is lower, people are incentivized to redeem their tokens against the DC. As a result, the total amount of tokens in circulation will drop, thus increasing the market value, up until the point in which the market value will match the redeem value.

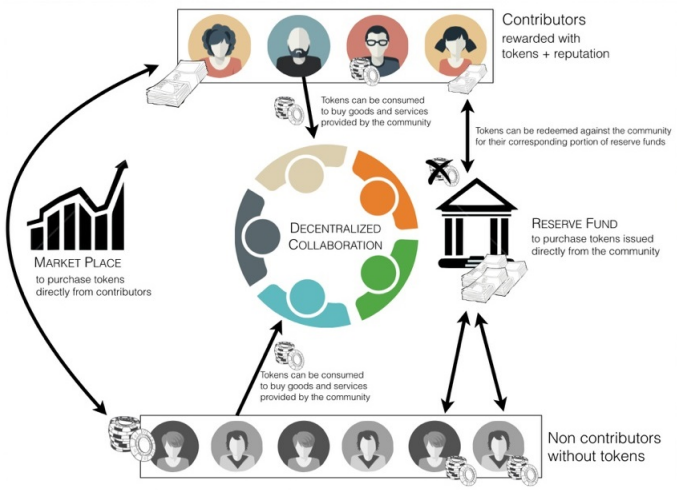

Figure 8: Decentralized Cooperation (Source: Pazaitis et al. 2017)

This sort of "decentralized cooperation" aims to coordinate and incentivize the production and consumption in a decentralized manner. Pazaitis et al. (2017) acknowledges that the blockchain based DC model is mostly theoretical and rests upon a superficial understanding of how it could in practice apply to real-world communities.

Given the early stage of the technology, there is no robust empirical evidence regarding the practical implementation of this model. However, blockchain has proved to be able to facilitate distributed value systems (e.g. bitcoin) with native tokens representing a generic and measurable unit of value. This is why the procedures to create new kind of value systems are worth taking a closer look at.

7 Discussion and Conclusions

The objective of this thesis is to provide an overview of the relevant published work related to the economics of blockchain. The research question is "What are the possible economic and institutional implications of blockchain?" In order to answer the question, a comprehensive overview of the topic is gained through a three-stage review process, which is explained in chapter 3 in more detail. The list of the major contributions to the topic and key themes can be found in table 1 in chapter 2. The possible implications are analyzed through the viewpoints of monetary and innovation economics and also from the governance point of view.

Rather than a single efficiency improving ICT, blockchain should be attached to the larger context of the digitalization of the economy. Digitalization is shaping the dynamics of governance, ownership, production, consumption and exchange.

Digital goods and services might be extremely beneficial and have high use value, but simultaneously they might have low transaction value, making it hard to incentivise optimal production. In addition, transaction costs and lack of trust are partly bottlenecks of the expansion of digital peer-to-peer platforms. Even though the technology is only taking its first development steps, it is clear that blockchain has features that could contribute to the unlocking of the digital economy's potential. This chapter summarizes and discusses the findings and suggests directions for the future research.

Monetary-Centered Approach

Blockchain can provide a technical infrastructure for designing new types of monetary systems that could potentially disrupt payment or even monetary systems (Böhme et al., 2015). Whereas historically currencies were chosen from among existing commodities, blockchain gives unprecedented flexibility to designing the attributes of currencies (Gans and Halaburda, 2015b).

Böhme et al. (2015) argue that blockchain is a social science laboratory for monetary economics. Digital money, like blockchain-enabled cryptocurrencies, gives flexibility to for example i) design and experiment various supply procedures, ii) build in decreasing or increasing nominal value to the design of the currency, or iii) incentivize certain kind of demand or production by designing the currency to be more valuable in certain activities or geographical areas, for example. These attributes can give entirely new tools for policymakers to design

and implement incentive structures and monetary policies.

Private digital currencies might also generate economic efficiency gains for several reasons. For example, international remittances, foreign exchanges and portability and divisibility properties of digital money are identified as potential sources of the blockchain enabled efficiency improvements (Dwyer, 2015; Peters and Panayi, 2016; Dandapani and Dandapani, 2017). Simultaneously, the supply should be made credibly scarce in order for the private money to maintain a positive value. In practice, this is created by coding an immutable supply procedure to the algorithm. However, if the money supply of a currency is fixed or decreasing, there might be deflationary pressure making it poor medium of exchange (Böhme et al., 2015).

Innovation-Centered Approach

The economic and institutional implications of blockchain will largely be affected by the scope of the diffusion of the technology. Maximization of profits is a powerful driver of technological change (Huesemann and Huesemann, 2011). From the innovation viewpoint, potential profits gained from investments determine the market-driven diffusion process.

Profits can be generated from two sources: cost savings through efficiency improvements and increased revenue through new marketplaces. The diffusion process can also be partly driven by exogenous, non-price drivers, including public support as well commons-oriented open source communities (Allen, 2016). In the case of blockchain, the efficiency gain is likely to be realized through organizational efficiency rather than more direct gains, like more efficient transfer of information. The declining production costs often derive from stripping out layers of activity that are no longer needed (Davidson et al., 2016b).

Blockchain also enables new marketplaces to emerge, which might generate profits and thus drive investments and technological development. Through a more cost-efficient and decentralized monitoring of the market participants, blockchain can facilitate exchange for items and services that were not efficient enough to be exchanged previously (Catalini and Gans, 2016). This could be the case in a market that requires a verification of trust and mechanisms to monitor reputation and payment systems, but in which the transaction value is low. In this kind of a situation, blockchain may be instrumental in creating profitable business models.

The concept of general-purpose technologies (GPTs) gives another interesting way to study the technological progress and innovation. Bresnahan and Trajtenberg (1995) suggest that GPTs are the ultimate source of productivity increases, and thus, long-run economic growth. Even though it is hard to predict ex-ante which technologies will fulfill the definition of a GPT, blockchain fulfill the three features of the definition: it is a pervasive technology which has scope for improvement and innovational complementarities. Thereby, for example Catalini and Gans (2016), Kane (2017) and Allen (2016) claim that the blockchain technology has the key features to become one.

Governance-Centered Approach

In chapter 6, the ability of blockchain to provide new instruments to prove economic interactions and decision-making are reviewed from the governance viewpoint. According to Davidson et al. (2016b) blockchain can facilitate trust for economies, where previously agents were technologically constrained to the types of economic governance that could be generated only by firms, organizations, markets and governments. Spread of blockchain technology would thereby imply a shift towards more decentralized and self-organizing economies. The utopian views of blockchain argue that blockchain will disrupt every market by eliminating the need for intermediation by facilitating trust. More realistically, Catalini and Gans (2016) argue that blockchain is "more likely to change the scope of intermediation" and to create new markets through the reduction of transaction costs.

The basic insight from the governance viewpoint is that blockchain has potential to facilitate a shift from firms towards markets. It can also decrease the need for trusted intermediaries (Davidson et al., 2016a). This could imply potentially more efficient use of economic institutions.

Even though the models of how blockchain could incentivize decentralized commons-oriented production are still mostly theoretical, Pazaitis et al. (2017) argue that the blockchain technology supports the polycentricity of value, fluid coordination and multiplicity of contributions in an inclusive joint production. This is important in communities that create goods and services with low transaction value but high use value like in many cases in the digital economy. Swan (2015) and Crosby et al. (2016) also characterize blockchain as a society's universal record-keeping system. It could play an important role in unlocking the full

potential of digital platforms.

Directions for the Future Research

The economic literature on blockchain is still in its infancy, but it is continuously developing. However, currently even the clear definition and terminology are lacking. This definitely creates challenges in accumulating scientific knowledge on the subject and in establishing a meaningful regulatory environment around it.

From the monetary viewpoint, the research on the different designs of cryptocurrencies and digital currencies in general is highly interesting since it could open up entirely new opportunities for creating economic and monetary policies for different purposes. Böhme et al. (2015) state that blockchain should be considered as a social laboratory for monetary policy. Indeed, there are many possibilities which can be easier experimented with digital money. The possible subjects of research could be, for example, what would be the impact of a currency that has a decreasing nominal value? What would happen if money would have different value in different activities?

From the innovational viewpoint, the evidence of the profitability of the blockchain business models is important for entrepreneurs to make investment decisions and thus drive the development of the technology. As Zhao et al. (2016) state, "business research in blockchain is found mainly at the conceptual level that conceptualizes blockchain innovations in business and at the prescriptive level that outlines business applications of blockchain". Thus, research on the exact source and dynamics of efficiency gains or the creation of new markets could be beneficial.

From the governance viewpoint, the economic incentives of blockchain in joint and open source production (like is the case with Backfeed) would also be beneficial to study. This would enhance the understanding of how the production, consumption and ownership in the digital knowledge economy should be organized in order to take advantage of its potential gains more effectively.

References

S. Adam. The theory of moral sentiments. *DD Raphael & AL MacFie (éd.)*, 6, 1759.

R. Ali, J. Barrdear, R. Clews, and J. Southgate. The economics of digital currencies. *Bank of England QUaterly Bulletin 2014 Q3*, 2014.

D. W. Allen. Discovering and developing the blockchain crypto-economy. *SSRN Working Paper*, 2016.

S. Athey, I. Parashkevov, V. Sarukkai, and J. Xia. Discovering and developing the blockchain crypto-economy. *Stanford University Graduate School of Business Research Paper No. 16-42.*, 2016.

bankofcanada.ca. Decentralized e-money (bitcoin). *Bank of Canada - Backgrounders, retrieved August 6, 2017, from http://www.bankofcanada.ca/wp-content/uploads/2014/04/Decentralize-E-Money.pdf*, 2014.

S. Barber, X. Boyen, E. Shi, and E. Uzun. Bitter to better—how to make bitcoin a better currency. In *International Conference on Financial Cryptography and Data Security*, pages 399–414. Springer, 2012.

J. Becker, D. Breuker, T. Heide, J. Holler, H. P. Rauer, and R. Böhme. Can we afford integrity by proof-of-work? scenarios inspired by the bitcoin currency. In *The Economics of Information Security and Privacy*, pages 135–156. Springer, 2013.

M. Bellare and P. Rogaway. Introduction to modern cryptography. *Ucsd Cse*, 207:207, 2005.

I. Bentov, A. Gabizon, and A. Mizrahi. Cryptocurrencies without proof of work. In *International Conference on Financial Cryptography and Data Security*, pages 142–157. Springer, 2016.

R. Böhme, N. Christin, B. Edelman, and T. Moore. Bitcoin: Economics, technology, and governance. *The Journal of Economic Perspectives*, 29(2):213–238, 2015.

T. F. Bresnahan and M. Trajtenberg. General purpose technologies 'engines of growth'? *Journal of econometrics*, 65(1):83–108, 1995.

V. Buterin. On bitcoin maximalism, and currency and platform network effects. *Retrieved August 6, 2017, from*

https://blog.ethereum.org/2014/11/20/bitcoin-maximalism-currency-platform-network-effects/, 2014.

K. I. Carlaw and R. G. Lipsey. Gpt-driven, endogenous growth. *The Economic Journal*, 116(508):155–174, 2006.

C. Catalini and J. S. Gans. Some simple economics of the blockchain. Technical report, National Bureau of Economic Research, 2016.

R. H. Coase. The nature of the firm. *economica*, 4(16):386–405, 1937.

Coinmarketcap.com. Crypto-currency market capitalizations. *Retrieved August 6, 2017, from https://coinmarketcap.com/all/views/all/*, 2017.

K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, et al. On scaling decentralized blockchains. In *International Conference on Financial Cryptography and Data Security*, pages 106–125. Springer, 2016.

M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman. Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2:6–10, 2016.

C. J. Dahlman. The problem of externality. *The journal of law and economics*, 22(1):141–162, 1979.

K. Dandapani and K. Dandapani. Electronic finance–recent developments. *Managerial Finance*, 43(5):614–626, 2017.

P. Dasgupta. Trust as a commodity. *Trust: Making and breaking cooperative relations*, 4:49–72, 2000.

S. Davidson, P. De Filippi, and J. Potts. Disrupting governance: The new institutional economics of distributed ledger technology. *SSRN Working Paper*, 2016a.

S. Davidson, P. De Filippi, and J. Potts. Economics of blockchain. *SSRN Working Paper*, 2016b.

W. Diffie and M. E. Hellman. Multiuser cryptographic techniques. In *Proceedings of the June 7-10, 1976, national computer conference and exposition*, pages 109–112. ACM, 1976.

S. C. Dow and P. E. Earl. *Money matters*. Robertson, 1982.

G. P. Dwyer. The economics of bitcoin and similar private digital currencies. *Journal of Financial Stability*, 17:81–91, 2015.

ECB. virtual currency schemes. *European Central Bank, retrieved from https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf*, 2012.

D. S. Evans. Economic aspects of bitcoin and other decentralized public-ledger currency platforms. *Coase-Sandor Institute for Law and Economics Working Paper No. 68*, 2014.

M. Friedman. The role of monetary policy. 1968.

J. S. Gans and H. Halaburda. Some economics of private digital currency. In *Economic Analysis of the Digital Economy*, pages 257–276. University of Chicago Press, 2015a.

J. S. Gans and H. Halaburda. Some economics of private digital currency. In *Economic Analysis of the Digital Economy*, pages 257–276. University of Chicago Press, 2015b.

Gartner. Gartner's 2016 hype cycle for emerging technologies identifies three key trends that organizations must track to gain competitive advantage. *Retrieved August 6, 2017, from http://www.gartner.com/newsroom/id/3412017*, 2016.

J. T. Holdsworth. *Money and banking*. Appleton, 1914.

M. Huesemann and J. Huesemann. *Techno-fix: why technology won't save us or the environment*. New Society Publishers, 2011.

M. Hufty. Investigating policy processes: the governance analytical framework. *SSRN Working Paper*, 2011.

W. S. Jevons. *Money and the Mechanism of Exchange*, volume 17. Kegan Paul, Trench, 1885.

R. Johnson. Blockchain adoption in capital markets. *Retrieved August 6, 2017, from https://www.greenwich.com/press-release/wall-street-blockchain-investments-top-1billion-annually-0*, 2016.

E. Kane. Is blockchain a general purpose technology? *SSRN Working Paper*, 2017.

N. Kiyotaki and R. Wright. On money as a medium of exchange. *Journal of Political economy*, 97(4):927–954, 1989.

Litecoin.org. Litecoin supply. *Retrieved August 6, 2017, from https://litecoin.org*, 2017.

loc.gov. Regulation of bitcoin in selected jurisdictions. *The Law Library of Congress, Global Legal Research Center. Retrieved August 6, 2017, from https:http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf*, 2014.

R. E. Lucas. On the mechanics of economic development. *Journal of monetary economics*, 22(1):3–42, 1988.

T. J. MacDonald, D. Allen, and J. Potts. Blockchains and the boundaries of self-organized economies: Predictions for the future of banking. *Available at SSRN 2749514*, 2016.

J. Mattila. The blockchain phenomenon. *Berkeley Roundtable of the International Economy*, 2016.

J. M. McNamara, P. A. Stephens, S. R. Dall, and A. I. Houston. Evolution of trust and trustworthiness: social awareness favours personality differences. *Proceedings of the Royal Society of London B: Biological Sciences*, 276(1657): 605–613, 2009.

E. C. Moreno. Bitcoin in argentina: Inflation, currency restrictions, and the rise of cryptocurrency. *University of Chicago Law School,International Immersion Program Papers.*, 2016.

S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Bitcoin Whitepaper*, 2008.

D. C. North. *Institutions, institutional change and economic performance*. Cambridge university press, 1990.

K. J. O'Dwyer and D. Malone. Bitcoin mining and its energy footprint. *China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014)*, 2014.

A. Pazaitis, P. De Filippi, and V. Kostakis. Blockchain and value systems in the sharing economy: The illustrative case of backfeed. *Technological Forecasting and Social Change*, 2017.

G. W. Peters and E. Panayi. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. In *Banking Beyond Banks and Money*, pages 239–278. Springer, 2016.

G. W. Peters, E. Panayi, and A. Chapelle. Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective. *SSRN Working Paper*, 2015.

M. Pilkington. Blockchain technology: principles and applications. *Browser Download This Paper*, 2015.

M. Raskin and D. Yermack. Digital currencies, decentralized ledgers, and the future of central banking. Technical report, National Bureau of Economic Research, 2016.

W. Roberds. Review of making money: Coin, currency, and the coming of capitalism by christine desan. *Journal of Economic Literature*, 54(3):906–921, 2016.

P. M. Romer. Increasing returns and long-run growth. *Journal of political economy*, 94(5):1002–1037, 1986.

P. M. Romer. Endogenous technological change. *Journal of political Economy*, 98(5, Part 2):S71–S102, 1990.

R. M. Solow. A contribution to the theory of economic growth. *The quarterly journal of economics*, 70(1):65–94, 1956.

Spendbitcoins.com. Over 100,000 merchants accept bitcoin. *Retrieved August 6, 2017, from http://spendbitcoins.com*, 2017.

M. Swan. *Blockchain: Blueprint for a new economy.* " O'Reilly Media, Inc.", 2015.

T. W. Swan. Economic growth and capital accumulation. *Economic record*, 32 (2):334–361, 1956.

T. Swanson. Great chain of numbers. *A Guide to Smart Contracts, Smart Property, and Trustless Asset Management, publisher: Creative Commons-Attribution 4.0 International*, 2014.

S. Tadelis. Reputation and feedback systems in online platform markets. *Annual Review of Economics*, 8:321–340, 2016.

O. E. Williamson. Markets and hierarchies. *New York*, pages 26–30, 1975.

O. E. Williamson. *The economic intstitutions of capitalism.* Simon and Schuster, 1985.

O. E. Williamson. Calculativeness, trust, and economic organization. *The Journal of Law & Economics*, 36(1):453–486, 1993.

D. Yermack. Corporate governance and blockchains. *Review of Finance*, 21(1): 7–31, 2017.

J. L. Zhao, S. Fan, and J. Yan. Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation*, 2(1):28, 2016.

G. Zyskind, O. Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE*, pages 180–184. IEEE, 2015.